IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF MISSOURI
WESTERN DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS TO AND FROM THE E-MAIL ACCOUNT IDENTIFIED AS ***"DAMAGEINCMD@GMAIL.COM"***	**UNDER SEAL** No. 18-SW-00041-JTM

AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR AUTHORIZATION OF THE INTERCEPTION OF ELECTRONIC COMMUNICATIONS

Your Affiant, Chris Tauai, Special Agent, United States Veteran Affairs, Office of Inspector General (VA-OIG), being duly sworn, does hereby depose and state as follows:

INTRODUCTION

1. This affidavit is in support of an application for a search warrant for information associated with accounts stored at premises owned, maintained, controlled, or operated by Google, Inc. (Google), an email provider headquartered at 1600 Amphitheatre Parkway Mountain View, CA 94043. The account to be searched is related to Michael Dingle also known as Patrick Michael Dingle to include, but not limited to damageincmd@gmail.com, further described in the following paragraphs and in **Attachment A**. As set forth herein, there is probable cause to believe on the computer systems of Google there exists evidence, fruits, and instrumentalities of violations of 18 U.S.C. § 1343 (wire fraud), 18 U.S.C. § 1001 (false statements), 18 U.S.C. § 371 (conspiracy to commit offense or to defraud the United States), 18 U.S.C. § 1031 (major fraud against the United States) and 18 U.S.C. §§ 1956 and 1957 (money laundering). This affidavit is made in support of

an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(a) and 2703(c)(1)(A) to require Google to disclose to the Government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications, and specified in **Attachment B** ("Items to be Seized"), which constitute contraband, instrumentalities and evidence of the foregoing violations.

2. This case is being investigated by VA-OIG, Defense Criminal Investigative Service (DCIS), Department of Army Criminal Investigative Division-Major Procurement Fraud Unit (Army CID-MPFU), Small Business Administration Office of Inspector General (SBA-OIG), General Service Administration Office of Inspector General (GSA-OIG), United States Department of Agriculture Office of Inspector General (USDA-OIG), Internal Revenue Service- Criminal Investigation (IRS-CI), and U.S. Secret Service (USSS).

AFFIANT BACKGROUND

3. I am a special agent with the VA-OIG, and have been so employed since April 2012. As such, I am a federal law enforcement officer of the United States empowered by law to conduct investigations of and make arrests for offenses enumerated in Title 18, United States Code. Prior to my employment at VA-OIG, from May 2007 to April 2012, I served as a special agent with USSS.

4. Throughout my career, I have investigated violations of local, state and federal criminal laws in general crimes, violent crimes, and white collar crimes.

5. I have gained experience through training, seminars, classes, and everyday work related to conducting these types of investigations. Based on my experiences, I am familiar with the techniques used by persons who are engaged in a wide variety of criminal activity.

6. I have personally participated in the investigation of the offenses referred to above which are relating to service-disabled veteran-owned small business (SDVOSB) fraud and Small Business Administration (SBA) 8(a) contract fraud conspiracy being executed by Michael Patrick Dingle also known as Patrick Michael Dingle (Dingle) and his associates to include Matthew Torgeson (Torgeson), Matthew McPherson (McPherson), Monica Haavig (Haavig), Stephon Ziegler (Ziegler), Rustin Simon (Simon), and Jacob Baucom (Baucom), by fraudulently using the companies Zieson Construction Company, LLC (Zieson), Simcon Corp (Simcon), and Onsite Construction Group, LLC (Onsite), to obtain government contracts set aside for legitimate SDVOSBs and minority-owned businesses when in fact, these companies were not entitled to those government set-aside contracts.

JURISDICTION

7. Title 18, United States Code, Section 2703(c)(A) allows for nationwide service of process of search warrants for the contents of electronic communications. Pursuant to 18 U.S.C. § 2703, as amended by the USA PATRIOT Act, Section 220, a government entity may require a provider of an electronic communication service or a remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service pursuant to a warrant issued using procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711, 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(I).

8. Title 18, United States Code, Section § 2703 further states in part:

> (a) Contents of Wire or Electronic Communications in Electronic Storage. A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communication system for more than one hundred and eighty days by the means available under subsection (b) of this section.
>
> (b) Contents of Wire or Electronic Communications in a Remote Computing Service.
>
> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection.
>
> (A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant....

9. Title 18, United States Code, Section 2703(c)(2) adds that a provider of an electronic communication service or remote computer service must also provide, without notice to the customer, the name, address, connection records, length of service, and means of payment pursuant to a search warrant.

10. This application seeks a warrant to search all responsive records and information under the control of Google, a provider subject to the jurisdiction of this court, regardless of where Google has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within Google's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States. [1]

PURPOSE OF THE APPLICATION

11. The purpose of this affidavit is to set forth facts establishing probable cause to support the issuance of the requested search warrant. The information contained in this affidavit is based either on my own personal knowledge or on information provided to me by other law enforcement officers. Not all facts known to me are necessarily contained in this affidavit. The affidavit is limited to the facts relevant and necessary to establish probable cause for the requested search warrant.

---

[1] It is possible that Google stores some portion of the information sought outside of the United States. In *Microsoft Corp. v. United States*, 2016 WL 3770056 (2nd Cir. 2016), the Second Circuit held that the government cannot enforce a warrant under the Stored Communications Act to require a provider to disclose records in its custody and control that are stored outside the United States. As the Second Circuit decision is not binding on this court, I respectfully request that this warrant apply to all responsive information— including data stored outside the United States— pertaining to the identified account that is in the possession, custody, or control of Google. The government also seeks the disclosure of the physical location or locations where the information is stored. The overwhelming number of district courts who have considered this issue after *Microsoft Corp*. have required the production of all responsive documents wherever found.

12. There is probable cause to believe the subjects of this investigation used email addresses including, but not limited to damageincmd@gmail.com in the commission and furtherance of the aforementioned fraud scheme. This email address was created and used with the intent to present, correspond, or communicate with the government to obtain contracts for Zieson, Simcon and Onsite. Examples of such use of this email address is presented below.

13. The facts set forth in this affidavit are based on personal knowledge I obtained and from others, to include other law enforcement officers involved in this case; through interviews and reviews of contract-related documents, electronic files, emails, grand jury subpoena returns, as well as other records and files related to this investigation. Since this affidavit is being submitted for the limited purpose of supporting an application for a search warrant, I have not included each and every fact known to me concerning this investigation, but set forth only those facts necessary to establish probable cause.

14. Based on my training and experience, I am familiar with the federal government acquisition and contracting process as well as the SDVOSB and other government set-aside programs.

SDVOSB PROGRAM

15. The United States Government sets aside contract benefits and offers preferential bidding status for SDVOSBs. Businesses vying for the SDVOSB status must be at least 51% owned by an individual who is a service-disabled veteran (SDV). This SDV must, among other requirements, manage and control the daily operations and long-term decision making of the business. Additionally, pursuant to federal regulations, the SDVOSB must be 'small' as determined by SBA. Once a business obtains this certification, it may compete for government issued contracts

exclusively set aside for SDVOSBs. However, if a SDVOSB exceeds the 'small' size requirement, it is no longer eligible to be awarded SDVOSB set-aside contracts.

8(a) BUSINESS DEVELOPMENT PROGRAM

16. The SBA administers the 8(a) Business Development Program (8(a) program) to assist small, disadvantaged businesses. This program is designed to assist socially and economically disadvantaged entrepreneurs gain access to the economic mainstream of American society and gain a foothold in government contracting. A host of eligibility requirements are in place to qualify for this program but the overriding qualifiers are that the business must be 51% or more owned by a socially and economically disadvantaged individual and this individual must also control and manage the daily operations of the business. Separate eligibility requirements exist for a business that is owned by a Native-American. Additionally, 8(a) firms must be 'small' as determined by SBA. SBA offers contracts set aside for award to business entities which qualify under the 8(a) program. However, if an 8(a) firm exceeds the 'small' size requirement, it is no longer eligible to be awarded SBA set-aside contracts.

FACTS ESTABLISHING PROBABLE CAUSE

17. VA-OIG and SBA-OIG opened this investigation based on information from an SBA employee assigned to a Simcon contract. In reviewing an email from Simcon, the SBA employee noticed that the metadata associated with the email indicated that while the email appeared to originate from Simcon, it had actually been sent from a Zieson server. The SBA employee raised the concern because Simcon would not have been eligible for the contract if Simcon had a relationship to Zieson due to Zieson's size.

18. Further, investigators received information from a confidential source of information (source) that Zieson was not managed or controlled by the SDV who

owned Zieson on paper. Instead, the source, an individual familiar with Zieson operations as a former Zieson employee who was directed to work on both Zieson and Simcon matters, indicated that Dingle, who is not an SDV, managed and controlled Zieson.

19. Neither Dingle, Torgeson, McPherson nor Haavig are SDVs or certified 8(a) minorities.

20. Ziegler and Baucom are believed to be SDVs and Ziegler and Simon are believed to be certified 8(a) minorities.

ZIESON FORMATION

21. Kansas Secretary of State, Missouri Secretary of State, and VA Center for Verification and Evaluation (CVE) records indicate Zieson was formed on July 9, 2009, and list Ziegler as a founding member and 52% majority owner. Torgeson was listed as a 48% owner. However, Torgeson later sold his shares to Ziegler on January 1, 2010. Zieson's Operating Agreement, dated July 28, 2010, listed Ziegler as the sole member with 100% membership interest. Records submitted to CVE by Zieson indicated Ziegler has an electrical journeyman's license and had never operated a general construction business before.

22. Kansas Department of Labor wage records indicated Ziegler worked at Torgeson Electric Company, Inc. (Torgeson Electric) in the first and second quarters of 2010.

23. In documents submitted to CVE by Zieson, Dingle is listed as Zieson's Operations Manager and Senior Project Manager. Dingle's resume contains extensive education and experience in operating general construction businesses.

24. Ziegler is believed to be an SDV and 8(a) certified minority. Dingle is neither an SDV nor a certified 8(a) minority.

25. Zieson's business address listed on their website is 1601 Iron Street, Suite 201, North Kansas City, Missouri 64116, which is in the same building and floor as Simcon and Onsite as described below.

ONSITE FORMATION

26. Records filed with the Missouri Secretary of State indicate Onsite was formed on January 20, 2010, in the state of Oklahoma with Baucom listed as the authorized person, but was registered in the state of Missouri by Dingle on May 17, 2017.

27. Baucom is believed to be an SDV. Dingle is not an SDV.

28. Onsite's business address listed on their website is 1601 Iron Street, Suite 209, North Kansas City, Missouri 64116, which is in the same building and floor as Zieson and Simcon as described herein.

SIMCON FORMATION

29. Records filed with the Missouri Secretary of State list Simon as the incorporator and registered agent of Simcon, which was formed on February 21, 2014. Simon filed a foreign for-profit corporation application with the state of Kansas on November 24, 2014.

30. Simon is believed to be a certified 8(a) minority.

31. Simcon's business address listed on their Facebook page is 1601 Iron Street, Suite 203, North Kansas City, Missouri, which is in the same building and floor as Zieson and Onsite.

32. Simon admitted in a sworn declaration that he was employed by Zieson from July 2011 until he allegedly ceased work with Zieson in October 2014.

1601 IRON STREET, NORTH KANSAS CITY, MISSOURI

33. A property records search revealed TDM Holdings, LLC, owns the property located at 1601 Iron Street in North Kansas City, Missouri, which is the business address for Zieson, Onsite and Simcon.

34. Records filed with the Kansas Secretary of State indicate TDM Holdings, LLC, was formed on July 3, 2014, and list Matthew McPherson as the registered agent and organizer. The latest annual report for TDM Holdings, LLC, filed on January 5, 2017, lists the following members as having 5% or more of capital in TDM Holdings, LLC: Matthew L. Torgeson Trust – C/O Matthew L. Torgeson, TTE; Michael P. Dingle; and CRM Investments, LC (CRM).

35. Records filed with the Kansas Secretary of State indicate CRM was formed on October 24, 2003. The latest annual report for CRM filed on January 9, 2017, lists the following members as having 5% or more of capital in CRM: Matthew C. McPherson and Mark R. McPherson.

36. McPherson Contractors, Inc. (McPherson Contractors) was formed in the state of Kansas in 1972. It was registered as a foreign corporation in Missouri in or about September 1983. The most recent annual registration filed with Missouri Secretary of State lists Matthew C. McPherson as President.

37. Records filed with the Missouri Secretary of State indicate Mets, LLC (Mets) was formed on February 12, 2010, and list Dingle as the registered agent and organizer.

38. Records filed with the Kansas Secretary of State indicate MLT Investments, LLC (MLT) was formed on October 31, 2011, and list Torgeson as the registered agent and organizer. It is believed that MLT stands for Matthew L.

Torgeson. Torgeson is the owner of Torgeson Electric, which is not a certified SDVOSB or 8(a) minority company.

39. A visual depiction of McPherson's, Torgeson's and Dingle's ownership and financial interests in the above-described entities is attached hereto as **Exhibit 1**.

40. It is believed that Dingle, Torgeson, McPherson and Haavig use the SDV and minority status of Simon, Ziegler, and Baucom, respectively, to organize allegedly SDV and minority-owned and controlled entities to compete for and obtain government set-aside contracts to which they are not entitled, thereby denying legitimate SDV and 8(a) minority owned and operated business concerns from being awarded the set-aside contracts.

41. Initial investigation revealed approximately 62 government-funded contracts totaling $317.9 million have been awarded, potentially due to fraud, to Zieson from 2009 to the present from agencies such as the United States Army (Army), VA, General Service Administration (GSA), and United States Department of Agriculture (USDA). The majority, if not all, of these contracts were set-aside as SDVOSB or 8(a). Based on financial analysis of Zieson's bank accounts, it appears that Zieson only receives income in connection with set-aside contracts involved in the scheme.

42. Initial investigation revealed approximately three government-funded contracts totaling approximately $12.5 million have been awarded, potentially due to fraud, to Simcon during fiscal years 2016 and 2017 from agencies such as Army and United States Air Force. The majority, if not all, of these contracts were set-aside as 8(a). Based on financial analysis of Simcon's bank accounts, it appears that

Simcon only receives income in connection with set-aside contracts involved in the scheme.

43. Initial investigation revealed approximately seven government-funded contracts totaling approximately $21.3 million have been awarded, potentially due to fraud, to Onsite since August of 2017 from agencies such as VA and GSA. The majority, if not all, of these contracts were set-aside as SDVOSB.

SIMCON'S RELATIONSHIP TO ZIESON

44. On or about February 9, 2017, SBA-OIG received information from a SBA business opportunity specialist indicating Simcon was awarded a contract worth approximately $8 million at Fort Leavenworth, Kansas; however, the SBA business opportunity specialist believed Simcon was related to a larger company, Zieson, based on metadata embedded in an email to SBA allegedly from a Simcon email account, and therefore should have been precluded from receiving the contract due to Zieson's large size.

45. As part of the bid proposal for the Fort Leavenworth, Kansas, solicitation from Simcon, Simon was listed as the president of the company and Dingle as operations manager. However, a pre-bid site visit sign-in sheet for this solicitation, dated August 16, 2016, showed Simon signed in under the organization name of "Zieson."

46. In a protest by the second lowest bidder regarding the Fort Leavenworth, Kansas, contract obtained by Simcon, Simon responded in a sworn declaration that he was the president of Simcon and had no affiliation with Zieson.

47. However, Simon signed Simcon's 2016 annual filing with the Kansas Secretary of State as President and listed 816-505-1695 as his contact phone number. That phone number is linked to Zieson.

48. From in or about March 2015 through in or about August 2016, while Haavig was receiving regular Zieson payroll deposits into her Platte Valley Bank account, Haavig also maintained and used a Simcon credit card account at CoreFirst Bank & Trust (CoreFirst).

49. In or about January 2015, Simcon submitted an application for a credit card account with CoreFirst. Simon signed the application as Simcon's President and Haavig signed as Simcon's Secretary.

50. That same month, Zieson submitted an application for a credit card account with CoreFirst. Ziegler signed the application as Zieson's Officer and Haavig signed as Zieson's Secretary, just as she had for Simcon.

51. On January 19, 2017, an email was sent to CoreFirst from Haavig's Zieson email account with her Zieson signature block stating in part, "**Simcon Corp** would like to order a credit card for" four named individuals. It should be noted that on December 2, 2016, just before this request, Simon declared in a sworn statement as part of the SBA appeal that "Zeison [sic] and Simcon are competitors. Zieson has no ownership, financial or management interest in Simcon."

52. Kansas Department of Labor records reveal that one of those individuals for whom a Simcon credit card was requested, Zieson Employee A, has been employed by Zieson since 2012. Another one of those individuals, Zieson Employee B, has been employed by Zieson since the second quarter of 2015.

53. On March 27, 2017, and again on July 11, 2017, emails were sent to CoreFirst from Haavig's Zieson email account with her Zieson signature block stating that Simcon wanted to order credit cards.

ZIESON

54. On or about June 13, 2017, the source was interviewed. The source worked for Zieson for approximately 20 months before being fired in approximately 2017. According to the source, Dingle is using the SDV and 8(a) minority status of Ziegler and Simon to obtain government set-aside contracts then steering a large portion of the work to non-SDVOSB subcontractors he is associated with such as Torgeson Electric. Additionally, the source advised that Ziegler and Simon do not run or oversee the day-to-day operations of Zieson and Simcon respectively, as required by SDVOSB and 8(a) regulations. The source indicated Ziegler and Simon occasionally stop in the office for brief periods to sign paperwork. The source further advised Dingle is the boss of Zieson and Simcon and "everyone" knows that Dingle "calls the shots." The source believed that Haavig was possibly an unnamed co-founder of Zieson and stated Haavig has been involved with Zieson from the beginning. The source further stated Haavig was the office manager for Zieson and continues to work for Zieson from Arizona where she now resides.

55. On requisite cover sheets attached to contract bids for Zieson, Dingle is listed as the Vice-President of the company. In addition, Dingle has signed several VA SDVOSB contracts listing his title as Operation Manager for Zieson. However, Dingle is not listed as a paid employee on Missouri or Kansas wage records for Zieson.

56. Records filed with the Missouri Secretary of State indicate Haavig and Associates, LLC (Haavig and Associates) was formed on December 21, 2007, and list Monica Haavig as the registered agent and organizer.

57. A Kansas Department of Labor wage record indicated Haavig was formerly employed by McPherson Contractors. She received wages from McPherson

Contractors from third quarter 2009 to second quarter 2010.

58. Haavig or Haavig and Associates began receiving funds from Mets in September of 2010. From September of 2010 through May of 2017, Haavig or Haavig and Associates received approximately $620,019 from Mets to include the following checks from Mets Platte Valley Bank account remitted in 2015 through 2017:

a. Two checks totaling $100,000, both remitted on December 24, 2015;

b. $250,000 check remitted on February 19, 2016; and

c. $100,000 check remitted on May 18, 2017.

At the time those checks were remitted from the Mets account, Zieson and Simcon deposits accounted for the overwhelming majority of deposits funding the Mets account at Platte Valley Bank.

59. Missouri employment records and Haavig's bank statements indicate Haavig worked for Zieson from approximately 2010 through at least the 1st quarter of 2017. Further, Kansas employment records indicate Haavig worked for McPherson Contractors in 2009 and 2010.

60. Upon review of Zieson's bank account records, two companies, Mets and MLT, belonging to Dingle and Torgeson respectively, were identified as receiving the majority of proceeds from the set-aside government contracts obtained by Zieson. Mets received approximately $5.8 million and MLT received approximately $2.8 million from approximately 2009 to date. However, Ziegler only received approximately $1 million in payments. Dingle and Torgeson, through their entities, are receiving more proceeds than Ziegler who must be the highest paid employee pursuant to SDVOSB requirements. Additionally, Torgeson Electric received approximately $24.8 million from approximately 2009 to date in what

appears to be subcontract work from Zieson. Further, McPherson Contractors has received approximately $6.3 million from Zieson. Approximately $3.7 million appears to be in the form of distributions as reflected in paragraphs 59 through 70 herein.

ZIESON AND SIMCON PAYMENTS TO McPHERSON, DINGLE AND TORGESON ENTITIES

61. From approximately February 2015 through approximately June 2017, McPherson Contractors (owned by McPherson), Mets (owned by Dingle) and Torgeson personally or his entity MLT received disbursements in the amount of $3,696,909 each from Zieson and Simcon accounts for a total of $11,090,727 in disbursements as identified herein:

62. On February 5, 2015, three sequential checks were remitted from Zieson's CoreFirst account x1454, to include:

a. Check 19790 payable to McPherson Contractors, Inc. in the amount of $450,000;

b. Check 19791 payable to METS, LLC in the amount of $450,000; and

c. Check 19792 payable to Torgeson Electric Co., Inc. in the amount of $400,000.

63. Also on February 5, 2015, three sequential checks were remitted from Simcon's CoreFirst account x3271, to include:

a. Check 10035 payable to McPherson Contractors, Inc. in the amount of $35,000;

b. Check 10036 payable to METS, LLC in the amount of $35,000; and

c. Check 10037 payable to Torgeson Electric Co., Inc. in the amount of $35,000.

64. In February 2015, three checks were remitted from Zieson's CoreFirst

account x1454, to include:

a. Check 19960 payable to Torgeson Electric Co., Inc. in the amount of $350,000 remitted on February 23, 2015;

b. Check 19993 payable to McPherson Contractors, Inc. in the amount of $300,000 remitted on February 27, 2015; and

c. Check 19994 payable to METS, LLC in the amount of $300,000 also remitted on February 27, 2015.

65. Approximately one year later, on February 17, 2016, three sequential checks were remitted from Zieson's Platte Valley Bank account x2022, to include:

a. Check 11203 payable to McPherson Contractors, Inc. in the amount of $655,700;

b. Check 11204 payable to METS, LLC in the amount of $655,700; and

c. Check 11205 payable to MLT Investments, LLC in the amount of $655,700.

66. A month later, on March 17, 2016, three sequential checks were remitted from Simcon's CoreFirst account x3271, to include:

a. Check 10167 payable to McPherson Contractors, Inc. in the amount of $30,000;

b. Check 10168 payable to METS, LLC in the amount of $30,000; and

c. Check 10169 payable to MLT Investments, LLC in the amount of $30,000.

67. On April 20, 2016, three checks in the same amount were remitted from Zieson's accounts, one from its Platte Valley Bank account x2022 and two sequential checks from its Core First account x1454, to include:

a. Check 11451 from the Platte Valley Bank account payable to

McPherson Contractors, Inc. in the amount of $255,700;

b. Check 22236 from the CoreFirst account payable to METS, LLC in the amount of $255,700; and

c. Check 22237 from the CoreFirst account payable to MLT Investments, LLC in the amount of $255,700.

68. On May 16, 2016, three checks in the same amount were remitted from Zieson's accounts, one from its Platte Valley Bank account x2022 and two from its CoreFirst account x1454, to include:

a. Check 11559 from the Platte Valley Bank account payable to McPherson Contractors, Inc. in the amount of $400,000;

b. Check 22298 from the CoreFirst Bank account payable to METS, LLC in the amount of $400,000; and

c. Check 22297 from the CoreFirst Bank account payable to MLT Investments, LLC in the amount of $400,000.

69. On February 22, 2017, three sequential checks were remitted from Zieson's Platte Valley Bank account x2022, to include:

a. Check 13307 payable to McPherson Contractors, Inc. in the amount of $564,643;

b. Check 13308 payable to Mets, LLC, Michael P Dingle D/B/A METS, LLC in the amount of $577,643; and

c. Check 13309 payable to MLT Investments, LLC in the amount of $589,643.

70. On March 14, 2017, three nearly sequential checks were remitted from Zieson's Platte Valley Bank account x2022, to include:

a. Check 13412 payable to McPherson Contractors, Inc. in the amount

of $800,000;

b. Check 13413 payable to METS, LLC, Michael P Dingle D/B/A METS, LLC in the amount of $787,000; and

c. Check 13415 payable to MLT Investments, LLC in the amount of $775,000.

71. On April 18, 2017, three sequential checks were remitted from Zieson's CoreFirst account x1454, to include:

a. Check 23824 payable to McPherson Contractors, Inc in the amount of $175,000;

b. Check 23825 payable to METS, LLC in the amount of $175,000; and

c. Check 23826 payable to MLT Investments, LLC in the amount of $175,000.

72. On June 28, 2017, three sequential checks were remitted from Simcon's CoreFirst account x3271, to include:

a. Check 10377 payable to McPherson Contractors, Inc., in the amount of $30,866;

b. Check 10378 payable to METS, LLC in the amount of $30,866; and

c. Check 10379 payable to MLT Investments, LLC in the amount of $30,866.

73. A review of Zieson bank records revealed from February 2015 through June 2017, Zieson paid TDM Holdings, LLC approximately $461,473.06. These payments appear to be for rent, likely for 1601 Iron Street in North Kansas City, Missouri.

ONSITE'S RELATIONSHIP TO DINGLE AND ZIESON

74. Records filed with the Missouri Secretary of State indicate that on May

30, 2017, approximately two weeks after Onsite was registered as a foreign limited liability company with Dingle as the registered agent and 1601 Iron Street, Suite 201, Kansas City, Missouri, as the business address, Onsite's registered agent was changed from Dingle to Baucom, an SDV, listing Baucom as President and changing the business suite number from 201 to 209.

75. A review of Zieson bank account records revealed a $100,000 payment to Onsite on June 28, 2017, a $250,000 payment on August 2, 2017 and a $150,000 payment on August 8, 2017.

76. Onsite's address listed on all three checks was 1601 Iron Street, Suite 209, North Kansas City, Missouri 64116. This is the same building as Zieson's and Simcon's business address.

SUBJECT EMAIL ACCOUNT
DAMAGEINCMD@GMAIL.COM

77. Records filed with the Missouri Secretary of State for Damage, Incorporated revealed Mike Dingle as the owner with an address of 4478 SW Hwy J, Trimble, Missouri 64492. An application for Reservation of Name was signed by Dingle on July 30, 2010.

78. An online database search through MxToolbox.com showed damageincmd@gmail.com with an IP address of 173.194.67.27 that belongs to Google.

79. An online database search through DomainBigData.com showed damageincmd@gmail.com was associated with "Micahel Dingle [sic], address 4478 SW Hwy J, Trimble, MO."

80. A WHOIS.ICANN.org look up for Zieson.com showed this domain to be registered to "micahel dingle" [sic] with an email of damageincmd@gmail.com.

81. Records obtained from GoDaddy.com, LLC, revealed damageincorporatedkc.com was registered to "micahel dingle" [sic] with email address damageincmd@gmail.com. Onsite-cg.com was billed to "micahel dingle" [sic] with email address damageincmd@gmail.com.

82. Records obtained from Platte Valley Bank of Missouri for Dingle's bank accounts ending in 1928, 2259, and 2424 revealed Dingle's listed email address to be damageincmd@gmail.com.

83. On or about January 25, 2016, an electronic transmission was made to the Federal Government, System for Award Management, representing that Simcon was classified as "small" for the associated NAICS code of 236220. Simon, not Dingle, was listed as the person making this certification and damagedincmd@gmail.com was listed as his email account even though this account was set up in Dingle's name. Zieson was last awarded a set-aside contract in approximately September 2016. Investigation revealed that due to Zieson's size, Zieson was no longer eligible to apply for set-aside contracts. As described in paragraphs 44 through 53 above, Simon made a statement under penalty of perjury in February 2017 that there was no relationship between Zieson and Simcon. The investigation has revealed that as Zieson faced increasing difficulty obtaining set-aside contracts, Dingle and his co-conspirators established Simcon in order to continue the scheme.

84. Records obtained from Land Rover Palm Beach for a Mets purchase of a 2016 Land Rover with co-buyer listed as Dingle on December 10, 2016 revealed his listed email address to be damageincmd@gmail.com.

85. Records obtained from SBA.gov for Simcon's business profile, established in 2014 and last updated on June 15, 2017, revealed a registration

email address of damageincmd@gmail.com. Additionally, the SBA contact person for Simcon is listed as "Rustin Simon, 627 SW Topeka Blvd, Suite A, Topeka, KS 66603-3287, phone: 816-728-8180."

86. Accordingly, it appears that damageincmd@gmail.com which is owned by Google is used not only as a contact address in communication with the federal government for Simcon set-aside contracts, but is also used by Mets, an entity controlled by Dingle which has no known business purpose yet has received in excess of $3,000,000 in under three years from both Zieson and Simcon accounts as identified in paragraphs 61 through 72 above.

SEARCH PROCEDURE

87. To facilitate seizure by law enforcement of the records and information described in Attachment A, this affidavit and application for search warrant seek authorization to permit employees of Google and its product Gmail.com to assist agents in the execution of this warrant. In executing this warrant, the following procedures will be implemented:

a. The search warrant will be presented to Google personnel who will be directed to isolate those accounts and files described in Section II of Attachment A;

b. To minimize any disruption of computer service to innocent third parties, Google employees and/or law enforcement personnel trained in the operation of computers will create an exact duplicate of the computer accounts and files described in Section II of Attachment A, including an exact duplicate of all information stored in the computer accounts and files described in Section II of Attachment A;

c. Google employees will provide the exact duplicate in electronic form of the accounts and files described in Section II of Attachment A and all information stored in those accounts and files to the agent who serves this search warrant; and

d. Law enforcement personnel will thereafter review all

information and records received from Google employees to determine the information to be seized by law enforcement personnel pursuant to Section III of Attachments A.

BACKGROUND REGARDING COMPUTERS, THE INTERNET, AND EMAIL

88. The term "computer" as is defined in 18 U.S.C. § 1030(e)(1), includes an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes a data storage facility or communications facility directly related to or operating in conjunction with such device.

89. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience and knowledge, I know the following:

a. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. To access the Internet, an individual computer user must subscribe to an access provider, which operates a host computer system with direct access to the Internet. The world wide web (www) is a functionality of the Internet which allows users of the Internet to share information;

b. With a computer connected to the Internet, an individual computer user can make electronic contact with millions of computers around the world. This connection can be made by any number of means, including modem, local area network, wireless and numerous other methods; and

c. Email is a popular form of transmitting messages and/or files in an electronic environment between computer users. When an individual computer user sends email, it is initiated at the user's computer, transmitted to the subscriber's mail server, then transmitted to its final destination. A server is a computer that is attached to a dedicated network and serves many users. An email server may allow users to post and read messages and to communicate via electronic means.

GOOGLE INC.

90. Based on my research, I have learned the following about Google:

a. Google is an American multinational technology company that specializes in Internet-related services and products, which include online advertising technologies, search engine, cloud computing, software, and hardware. In 2004, Google launched Gmail. Gmail.com is an email service which is available free of charge to Internet users. Subscribers obtain an account by registering on the Internet with Gmail.com. Gmail.com requests subscribers provide basic information, such as name, birthday, gender, zip code, registration email address and other personal/biographical information. However, Gmail.com does not verify the information provided;

b. Gmail.com maintains electronic records pertaining to the individuals and companies for which they maintain subscriber accounts. These records include account access information, email transaction information, and account application information;

c. Subscribers to Gmail.com may access their accounts on servers maintained and/or owned by Google from any computer connected to the Internet located anywhere in the world;

d. Any email sent to a Gmail.com subscriber is stored in the subscriber's "mail box" on Gmail.com's servers until the subscriber deletes the email or the subscriber's mailbox exceeds the storage limits preset by Gmail.com. If the message is not deleted by the subscriber, the account is below the maximum limit, and the subscriber accesses the account periodically, that message can remain on Gmail.com's servers indefinitely;

e. When the subscriber sends an email, it is initiated at the user's computer, transferred via the Internet to Gmail.com's servers, and then transmitted to its end destination. Gmail.com users have the option of saving a copy of the email sent. Unless the sender of the email specifically deletes the email from the Gmail.com server, the email can remain on the system indefinitely. The sender can delete

the stored email message thereby eliminating it from the email box maintained at Gmail.com, but that message will remain in the recipient's email box unless the recipient deletes it as well or unless the recipient's account is subject to account size limitations;

f. A Gmail.com subscriber can store files, including emails and image files, on servers maintained and/or owned by Google;

g. A subscriber to Gmail.com may not store copies on his/her home computer of emails and image files stored in his/her Gmail.com account. The subscriber may store emails and/or other files on the Gmail.com server for which there is insufficient storage space in the subscriber's computer and/or which he/she does not wish to maintain in the computer in his/her residence. A search of the files in the computer in the subscriber's residence will not necessarily uncover the files the subscriber has stored on the Gmail.com server;

h. As a federal agent, I am trained and experienced in identifying communications relevant to the crimes under investigation. The personnel of Google are not. I also know the manner in which the data is preserved and analyzed may be critical to the successful prosecution of any case based upon this evidence. Computer Forensic Examiners are trained to handle digital evidence. Google employees are not. It would be inappropriate and impractical, for federal agents to search the vast computer network of Google for the relevant account and then to analyze the contents of the account on the premises of Google. The impact on Google's business would be severe;

i. To accomplish the objective of the search warrant with a minimum of interference with the business activities of Google, to protect the rights of the subject of the investigation and to effectively pursue this investigation, authority is sought to allow Google to make a digital copy of the entire contents of the information subject to seizure specified in Section II of Attachment A. That copy will be provided to me or to any authorized federal agent. The contents will then be analyzed to identify records and information subject to seizure pursuant to Section III of Attachment A; and

j. Executing a warrant to search a Gmail.com email account requires an approach similar to the standard approach for executing a warrant to search papers stored in a file cabinet. Searching the subject email account in this case for evidence of the target crimes will require that agents cursorily inspect all emails produced by Google in order to ascertain which contain evidence of those crimes, just as it is necessary for agents executing a warrant to search a filing cabinet to conduct a preliminary inspection of its entire contents to determine the documents which fall within the scope of the warrant. In addition, keyword searches alone are inadequate to ensure that law enforcement can discover all information subject to seizure pursuant to Section III of Attachment A. Keywords search text of common electronic mail, database and spreadsheet applications files (which files may have been attached to electronic mail) do not store data as searchable text.

STORED WIRE AND ELECTRONIC COMMUNICATION ACCESS

91. Title 18, United States Code, Chapter 121, Sections 2701 through 2711, is entitled "Stored Wire and Electronic Communications and Transactional Records Access."

a. Title 18, United States Code, Section 2703(a) provides, in part:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

b. Title 18, United States Code, Section 2703(b) provides, in part:

> (1) A governmental entity may require a provider of remote computing service to disclose the contents of any electronic

communication to which this paragraph is made applicable by paragraph 2 of this subsection –

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued under the Federal Rules of Criminal Procedure or equivalent State warrant...

(2) Paragraph 1 is applicable with respect to any electronic communication that is held or maintained on that service –

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
(B) Solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

c. The Government may also obtain records and other information pertaining to a subscriber to or customer of electronic communication service or remote computing service by way of a search warrant. 18 U.S.C. § 2703(c)(1)(A). No notice to the subscriber or customer is required. 18 U.S.C. § 2703(c)(3).

d. Title 18, United States Code, Section 2711, provides, in part:

As used in this chapter –

(1) the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section; and

(2) the term "remote computing service" means the provision to the public of computer storage or processing services by means of an electronic communications system.

e. Title 18, United States Code, Section 2510, provides, in part:

> (1) "contents," when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; . . .
>
> (2) "electronic communications system" means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications; . . .
>
> (3) "electronic communication service" means any service which provides to users thereof the ability to send or receive wire or electronic communications; . . .
>
> (4) "electronic storage" means –
>
> (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and
>
> (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.

CONCLUSION

92. Based upon the information above, I have probable cause to believe that on the computer systems owned, maintained, and operated by Google, headquartered at 1600 Amphitheatre Parkway Mountain View, CA 94043; and in particular, within files associated with the email account related to damageincmd@gmail.com there exists evidence, fruits, and instrumentalities of violations of Title 18, United States Code, including specifically § 1343, 1001, 371, 1031, 1956 and 1957.

93. Pursuant to Federal Rule of Criminal Procedure 41 and 18 U.S.C. § 2703, and by this affidavit and application, I request that the Court issue a search warrant directed to Google allowing agents to seize the email and other information stored on the Google servers for the computer accounts and files and following the search procedure described in Attachment A.

Special Agent Chris Tauai
VA-OIG

Sworn to before me and subscribed in my presence this
12th day of February 2018.

Sarah W. Hays
United States Magistrate Judge